

As to claims 10-18, 20-24 and 26-29, the final rejection does not appear to address any reasons for not allowing these claims. Accordingly, if these claims are not allowable, Applicants respectfully submit that the finality of the Office Action must be withdrawn since Applicants were not given any notices to the basis for the reasons for rejection for these claims in view of Applicants' previous responses.

Claims 1-4, 6, 8-18, 20-24 and 26-29 again stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis in view of an Ellison article entitled "Generalized Certificates". Applicants' invention is directed to a method and apparatus for providing updated digital signature key pairs to a plurality of clients in a public key system, as set forth for example, in the preamble of claim 1. As noted in Applicants' specification, if a key pair expires prior to being updated, information can be lost or no longer accessible. It is desirable to have a smooth transition from old to new encryption key pairs during the updating process and for assigning key pairs so changes do not cause unnecessary loss of access to information. Also fixed default periods for key expiry periods for all clients in the system are typically done in conventional public key cryptographic systems. Applicants have made numerous attempts to note that the teachings of Ellison that are cited are not related to Applicants' problem and are not related to providing updated digital signature key pairs to a plurality of clients in a public key system. Applicants, in previous responses, have also noted that the Office Action does not appear to provide any motivation to combine selective teachings of the cited references. In addition, Applicants have noted that it does not appear that the cited teachings of Ellison have been enabled as required by law. Applicants respectfully request a response to this assertion since it does not appear to have been addressed by the Examiner. (See for example Amendment After Final dated September 4, 2001).

In addition, it appears and as noted in previous responses, that impermissible hindsight is being used to combine disparate teachings of the references in an effort to render obvious Applicants claim invention. Applicants respectfully submit that the selective teachings of different references can only be combined if there is some suggestion or incentive to do so. Particular findings must be made as to the reason for the skilled artisan, with no knowledge of the claimed invention, would have selected specific components for combination in the manner claimed. Applicants have noted in several responses that the rejection does not appear to provide any factual support for any motivation to combine the system of Lewis which is directed to a system wherein each time a key request is performed, an active public key is discarded by using a key replacement message signed by an active private key and replacement private key, with selective teachings from the Ellison article regarding CRLs. Ellison teaches away from using certificate revocation lists and teaches away from using certification authorities to issue certificates. The Examiner admits that Lewis does not teach certificates with expiry data that are “user selectable” (even though Applicants do not claim user selectability), but also attempts to combine a reference that relates to a public key replacement system (Lewis) with the Ellison reference even though Ellison does not relate to Applicants’ claimed invention which is directed to a method for providing updated digital signature key pairs to a plurality of clients.

Applicants wish to clarify the record for purposes of getting the claims allowed or in the alternative, appealing to a higher authority if necessary. Applicants also note that the rejection uses impermissible selectivity of teachings even within the Ellison reference. For example, the rejection states that “Ellison talks throughout his disclosure about certificates, which are used to authenticate public keys. Certification authorities issues these certificates. On page 5, Ellison says that he believes that there is a problem with CRLs.” Applicants note that although not

indicated by the Examiner, Ellison actually teaches away from and discourages the use of certification authorities. As stated for example on page 4 of the Ellison article, Elliston states "This means that in most cases, there is not need for a formal Certification Authority (whose existence is devoted to assuring the binding between a physical person and a public key)." As such, the Examiner asserts that the Ellison reference has been cited because it teaches using certification authorities, however, Applicants respectfully note that Ellison when read in its entirety actually teaches away from using certification authorities and his main subject is that of generalized certificates and the non use of CRLs which is in his opinion, are ineffective or useless. Again, Applicants are unsure and again question how eliminating CRLs relates to Applicants' problem or invention since Applicants' invention, as noted in the preamble of the claims, is directed to, among other things, a method for providing updated digital signature key pairs to a plurality of clients. Since there does not appear to be any motivation to combine disparate teachings from unrelated references, Applicants respectfully submit that the claims are in condition for allowance.

Applicants also respectfully note that the Examiner's apparent reason for combining the references is that both references discuss differing aspects of public key based systems. However, Applicants respectfully submit that at issue are the specific teachings selectively chosen from these references since there is no motivation to combine such teachings.

Again, Applicants' invention is related to when to roll over keys which should occur prior to the invalidity of a certificate to avoid for example the ability of a user to access information or digitally sign information. In addition, the invention is related to providing selectable expiry data that is associated with one key pair, and associating that same expiry data

to a new key pair as set forth for example in the claims. Neither Lewis nor the Ellison article describe such methods or structure.

Also as noted above with respect to the Ellison reference, the problem faced by Ellison is completely different from the problem being addressed by Applicants' invention, Ellison does not address rolling over keys or updating key pairs and in addition, teaches away from, for example, a multi-client manager unit as claimed, since Ellison, among other things, teaches to avoid using certification authorities or other multi-client manager operations. In fact, Ellison's system would let an invalid certificate apparently roam the system and have the user or another non multi-client manager unit issue a certificate. In any event, Applicants note that the generalized certificate discussion and the elimination of CRLs is unrelated to Applicants updating of key pairs and as such, there is no motivation to combine selective teachings of these references with one another. In addition, neither reference describes, among other things, digitally storing both selected public key expiry data and selected private key expire data for a plurality of clients for association with a new digital signature key pair and associating the stored selected expiry data with a new digital signature key pair to effect a transition from an old digital signature key pair to a new digital signature key pair. The Office Action admits Lewis does not say that there are certificates with expiry data that is user selectable. For argument sake, Applicants again reassert the relevant remarks made in previous responses and that the Office Action mischaracterizes the claim language by indicating the expiry data as "user selectable" since the claim requires the opposite.

Applicants respectfully reassert the remarks made in previous responses with respect to the above claims.

For example, claim 2 requires, *inter alia*, that the selectable expiry data digital signature certificate lifetime data for variably setting a lifetime end date for digital signatures associated with a given client. However, as noted above, Ellison teaches away from the claimed invention and does not indicate that the selectable expiry data as provided through a multi-client unit, but in fact, indicates that such multi-client manager units are undesirable. Ellison also does not state that the data is selectable on a per client basis and in fact teaches a distinctly unrelated system. Accordingly, this claim is believed to be in condition for allowance.

As to claim 3, Applicants have requested a showing of the claimed privilege control mechanism as claimed as early back as September 7, 2000 and as yet has not received a specific showing that would contradict Applicants' assertion that the cited portion of Lewis merely states that the key service sends a key replacement message to each node or broadcasts a single key replacement message. The cited portion of Lewis does not mention the privilege control as claimed. Accordingly, this claim is believed to be allowable, but if the Examiner maintains his position, Applicants again respectfully request a showing as to where the Lewis reference teaches the privilege control mechanism as claimed.

As to claim 6, the Final Office Action indicates that these limitations are inherent in Ellison. Applicants respectfully reassert the remarks made with respect to Ellison in this response and in previous responses and notes that Ellison is silent as to a multi-client manager unit have, *inter alia*, a user interface that facilitates setting of a selectable expiry data on a per client basis to a desired date and Applicants respectfully requests factual support for the allegation that it is inherent. For example, Ellison does not teach a multi-client manager unit as claimed provide the selectability and storing and associating of the keys to renew public key

pairs as claimed. Accordingly, Applicants respectfully submit that this claim is also in condition for allowance.

Claims 5, 19, 25 and 27-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to claims 1, 14 and 21 above and further in view of Applicants submitted prior art.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Lewis and Ellison as applied to claim 1. Applicants respectfully reassert the remarks made above with respect to above claims 1, 14 and 21.

As to claim 5 for example, the Office Action takes official note that fixed length renewal periods are old and well known. The Office Action then concludes that it would have been obvious to set key update periods that are based on a fixed number of days and a percentage of a key's lifetime. Applicants respectfully submit that this is a mischaracterization of Applicants' claimed invention. Applicants note that conventional public key cryptographic systems typically have a fixed default period that is the same for all clients on the system. The default period is fixed and it is typically not adjustable by a multi-client manager or certification authority as claimed. However, Applicants claim, *inter alia*, initiating, by a client unit, digital signature key pair update requests based on whether differences between a current date and a digital signature private key lifetime end date is less than an absolute predetermined period of time, and based on whether the difference between a current date and a digital signature private key lifetime end date is less than a predetermined percentage of a total duration of a digital signature private key lifetime when the digital signature private key lifetime was selectable on a per client basis through a multi-client manager unit. No such digital key pair update request or basis for such a

request is taught or suggested in any of the references cited. It is Applicants' own disclosure which teaches such an invention which provides many advantages over conventional systems. Applicants respectfully request a showing of a teaching and references of such a digital signature key pair update request and the basis for initiating such a request as claimed.

Applicants respectfully submit that the claims are in condition for allowance and a Notice of Allowance is respectfully solicited. The Examiner is invited to contact the below-listed attorney if the Examiner believes that a conference would expedite the prosecution of the instant application.

Dated: November 8, 2002

Respectfully submitted,

By: 
Christopher J. Reckamp
Registration No. 34,414

Vedder, Price, Kaufman & Kammholz
222 N. LaSalle Street, Suite 2600
Chicago, IL 60601
PH: (312) 609-7599
FAX: (312) 609-5005